**IT Applications Unit 3, AOS 1, Online Communities**

1. Complete the following, from pgs, 32: **Network security**

**Networks are classified according to below and we will study the following:**

1. Network Categories: LAN, WAN
2. Network Architecture, client-server; peer-to-peer; internet peer-to-peer; intranet
3. Network communication standards
4. Network hardware and software
5. Transmission media
6. **Network security**
7. What types of physical security measures can be put in place?

Physical security measures, such as locks and alarms to warn of intruders, can protect a cabled network to a degree, but is can’t protect is from attack over the Internet.

**Usernames and passwords**

1. Recommend a password strategy that an organisation could use to avoid unauthorised access to the network.

* Be at least eight digits long
* Include non – alphabetical characters
* Not be easily guessed
* Be changed every month

**Firewall**

1. Describe the nature of a firewall.

A firewall is a server and software combination that filters the information coming through an Internet connection into an organisation’s internal network.

1. What are the main purposes of firewalls and how are these purposes achieved?

The filters used by a firewall include examining the IP address of computers that request information from an internal server, blocking all access to certain domain names, banning certain protocols from accessing particular.

1. Why do firewalls use 2 separate NICs?

One is connected to the internal network and the other to the outside world.

**Malware protection**

1. What is malware and what strategies are used to protect against this type of software?

Malware refers to malicious software and includes spyware, adware. Trojan horses, worms and viruses. Network administrators usually require workstations to run virus protection software.

**Encryption**

1. What is encryption?

Encryption is the process of translating data into a secret code that can only be read by authorised users.

1. Describe the nature of WPA or WPA2.

WPA or WPA2 is a security protocol for use by wireless LANs. It provides security by encrypting data sent over radio waves so that it is protected during transmission from the sending device to the receiving device.

1. What is encrypted data known as?

Encrypted data is known as ciphertext.

**Secure Websites**

1. Describe the secure protocol to allow secure financial transactions across the internet.

Websites that allow financial transactions use the industry standard hypertext transfer protocol security as the secure protocol between a client’s between browser and the web server, to ensure that a secure connection is established and maintained.

1. What is digital identification certificate technology based on?

Digital identifications certificate technology is based on a trusted certificate authority such as VeriSign Incorporated.

1. Describe the nature of Secure sockets layer (SSL) protocol.

SSL is a cryptographic protocol that provides secure connection on the Internet. When a web browser pints to a secured domain, a SSL “handshake” authenticates the server and the client key, and secure transmission can begin.

**Physical design of networks**

1. What is the role of a network diagram?

A network diagram is schematic method of showing the physical devices and communications lines present in a network.